UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF COMPUTER SERVERS AND RECORDS OF MICROSOFT INCORPORATED FOR INFORMATION ASSOCIATED WITH E-MAIL ACCOUNT	)))))	Case No.: 1:20-mj- 204-01-AJ UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, JON P. BENTSEN, being first duly sworn, hereby state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent employed by the Office of Export Enforcement (OEE), Bureau of Industry and Security ("BIS"), of the United States Department of Commerce. I have been employed as a Special Agent with the United States Department of Commerce since July 2020. Prior to that, I was employed as a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI") since April 2008 in their Key West, FL, New York, NY, and Boston, MA Field Offices, and have been a part of multiple investigations involving various federal crimes. I am authorized to make arrests for violations of federal law and I am familiar with the means by which individuals use computers and information networks to commit various crimes.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the individuals and entities listed below, and others, are violating the International Emergency Economic Powers Act, in violation of 50 U.S.C. §§ 1702 and 1705, and the Export Control Reform Act, 50 USC § 4819 by conspiring to export U.S.-origin goods to the Advanced Engineering Research Organization (AERO), an entity in Pakistan currently on the Bureau of Industry and Security Entity List, and as such, denied from receiving such goods. Their activities are also potential violations of 13 U.S.C. § 305 (unlawful export information activities),

18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 554 (outbound smuggling), 18 U.S.C. § 1001 (false statements), and 18 U.S.C. § 1956 (money laundering) (further referred to as the "Subject Offenses.")

3. The individuals and entities listed below, as well as their last known addresses, function as illicit procurement agents that seek to use intricate networks to acquire U.S.-origin commodities for AERO in violation of the Subject Offenses:

a. Omair Awan, Office No 60, Street 4, G-15/4, Islamabad, Pakistan

b. Rakhman Gul, Office No 60, Street 4, G-15/4, Islamabad, Pakistan

c. Kamran Hasan, Lub Thatoo, Hazra Rd., Tehsil Hasanabdal, Distt Attock, Islamabad, Pakistan

d. Sajid Hussain, Lub Thatoo, Hazra Rd., Tehsil Hasanabdal, Distt Attock, Islamabad, Pakistan

e. Sikandar Zulqarnain, Lub Thatoo, Hazra Rd., Tehsil Hasanabdal, Distt Attock, Islamabad, Pakistan

f. Mohammad Shafi, Lub Thatoo, Hazra Rd., Tehsil Hasanabdal, Distt Attock, Islamabad, Pakistan

g. United Enterprises, Mohra Chowk, Hazara Road, Hassan Abdal, District Attock, Pakistan

h. Quantum Logix (Private) Limited, Plot No 22, Sector H-9, Islamabad, Pakistan

i. Ramtech, Office No 60, Street 4, G-15/4, Islamabad, Pakistan

j. Spear Technology General Trading, PO Box 15693, Ajman, UAE

4. I submit this affidavit in support of an application for a warrant under 18 U.S.C. § 2703(a) and Rule 41 of the Federal Rules of Criminal Procedure to search and seize records and data from the e-mail account identified as omairawan@hotmail.com ("TA" or "the Target

Account") (as described in Attachment A).

5. I have probable cause to believe that this account contains evidence, fruits, and instrumentalities of the crimes identified above, as described in Attachment B.

6. Based on the e-mail address's domain name, I have probable cause to believe that the account and relevant data are maintained by Microsoft, Inc., which government databases indicate, accepts service of process at 1025 La Avenida, Mountain View, California, as described in Attachment A.

7. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

RELEVANT LAW

8. Under the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1707, the President of the United States was granted authority to deal with unusual and extraordinary threats to the national security, foreign policy, or economy of the United States. 50 U.S.C. § 1701(a). Pursuant to that authority, the President may declare a national emergency through Executive Orders that have the full force and effect of law. Among other things, IEEPA empowers the President to issue regulations governing exports from the United States.

9. On September 18, 2014, acting under the authority of IEEPA, the multi-agency body known as the End-user Review Committee (ERC) "determined to add Pakistan's Advanced Engineering Research Organization (AERO) and entities working with AERO to the Entity List for their involvement in activities contrary to the national security and foreign policy interests of the United States related to the illicit export, reexport and transfer (in-country) of items subject to

the EAR to unauthorized end users in Pakistan as described in § 744.11(b)(5) of the Export Administration Regulations (EAR, 15 CFR §§730-774). These entities' involvement in the procurement of sensitive U.S. technology in support of Pakistan's development of its missile and strategic unmanned aerial vehicle (UAV) programs is in violation of § 744.3 of the EAR, which requires a license to export, reexport or transfer (in-country) any item subject to the EAR that the exporter, reexporter, or in-country transferor knows will be used in the design, development, production or use of rocket systems by a country listed in the EAR's Country Group D:4 in Supplement No. 1 to part 740, in which Pakistan is included."[1]

10. In furtherance of the restrictions on AERO, on January 18, 2018 BIS added the alias "Integrated Solutions" at Lub Thatoo, Hazara Road, The Taxila District, Rawalpindi, Pakistan as an AKA for AERO to the entity list. This addition also added an alternate address for AERO of 53/2 26th Street, near Badara Commercial Area Phase 5 Extension, DHA Karachi, Pakistan.

11. I know from my training and experience that Pakistan's unregulated nuclear and UAV programs regularly employ a network of individuals and companies in third countries in order to obscure the ultimate end-user of commodities as well as the source of payment for the same. In fact, as part of the addition of AERO to the BIS Entity List, it was published that "Since 2010, Pakistan's AERO has used intermediaries and front companies to procure U.S.-origin items by disguising the end-uses and end-users of the items from U.S. exporters thereby circumventing BIS licensing requirements," and that "AERO has procured items on behalf of Pakistan's Air Weapons Complex (AWC), a Pakistani government entity responsible for Pakistan's cruise missile and strategic UAV programs."

[1] As published in The Federal Register on September 19, 2014, 79 FR 55998, pages 55998-56009.

12. Under IEEPA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued pursuant to the statute. 50 U.S.C. § 1705(a). Willful violations of the EAR constitute criminal offenses under IEEPA, and carry a 20-year maximum term of imprisonment and up to a $1,000,000 fine. 50 U.S.C. § 1705(c). Accordingly, an export that was completed or attempted with the intent that it would be ultimately destined for AERO or the Pakistan AWC would be in violation of IEEPA.

13. On August 13 2018, the President signed into law the National Defense Authorization Act of 2019, which includes the above-referenced Export Control Reform Act of 2018 ("ECRA"). In part, ECRA provides permanent statutory authority for the Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774, which most recently had been operative under the International Emergency Economic Powers Act, 50 U.S.C. § 1701-1706 ("IEEPA"). Accordingly, ECRA is the controlling statute (as the authority to promulgate export control regulations) for conduct occurring after August 13, 2018.

14. ECRA provides that "the national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specified activities of United States persons, wherever located, be controlled." ECRA § 1752. To that end, and like IEEPA before it, ECRA grants the President the authority to "(1) control the export, reexport, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or foreign persons; and (2) the activities of United States persons, wherever located, relating to" specific categories of items and information. ECRA § 1753. ECRA grants to the Secretary of Commerce the authority to establish the applicable regulatory framework.

15. Pursuant to that authority, the Department of Commerce reviews and controls the export of certain items, including goods, software, and technologies, from the United States to

foreign countries through the EAR. In particular, the EAR restrict the export of items that could contribute to the military potential of other nations or that could be detrimental to United States foreign policy or national security. The EAR impose licensing and other requirements for items subject to the EAR to be lawfully exported from the United States or lawfully re-exported from one foreign destination to another.

16. The most sensitive items subject to EAR controls are identified on the Commerce Control List, 15 C.F.R. § 774, Supp. No. 1, and are categorized by Export Classification Control Numbers, each of which has export control requirements depending on the destination, end use, and end user.

17. Under ECRA, it is unlawful for any person to violate, attempt to violate, conspire to violate, or cause a violation of its provision or any regulation, order, license, or other authorization issued under ECRA. ECRA § 1760. A person who willfully commits or willfully aids and abets these offenses is guilty of a federal crime punishable by up to a $1,000,000 fine and 20 years' imprisonment. ECRA § 1760(b).

18. I am also aware from my training and experience that entities such as AERO employ mechanisms by which they obfuscate the source of payments for commodities destined for companies and individuals on the BIS Entity List. Violations of IEEPA are "specified unlawful activities" as defined in 18 U.S.C. § 1956. Therefore, an attempt to "disguise the nature, the location, the source, the ownership, or the control of the proceeds" or transferring funds from outside the United States to inside the United States may violate the money laundering statute.

19. Moreover, some of the information contained in this affidavit comes from the review of the Automated Export System (AES) database maintained by U.S. Customs

and Border Protection. AES contains information provided to the United States Department of Commerce in the form of Electronic Export Information (EEI) forms. These forms must be filed by parties to the transaction that are in the United States, such as the seller or shipping company (15 CFR § 30.3), and contain information about all of the parties involved in the transaction. Providing false information, or causing false information to be provided to the United States Department of Commerce on an EEI, is a violation of 13 U.S.C. § 205 and 18 U.S.C. § 1001.

PRIOR WARRANT

20. This court, on August 18, 2020, issued a search warrant for Google, Inc. for contents of e-mail account rakhmangul@gmail.com as well as AERO accounts procurement.log@gmail.com and shipment.log@gmail.com. Information contained in this affidavit comes in part from the data returned by Google pursuant to that warrant. Non-Disclosure Orders issued by this court have been extended and are in force at the date of this affidavit.

CONSPIRACY TO OBTAIN AEROSPACE COMMODITIES IN NEW HAMPSHIRE

21. A previous investigation revealed that Microdaq, a U.S. company located in Contoocook, NH, conducted business and exported product to a company called "Product Engineering" in Rawalpindi, Pakistan on or about December 20, 2016. It was discovered that "Product Engineering" was in fact an additional alias name for AERO. As such AERO caused the export of electronic components valued at approximately $6,516.00 in violation of IEEPA.

22. Cooperating company A ("CCA") is an aerospace and defense contractor located in Bedford, NH. U.S. Government export records, and employees of CCA confirmed, that prior to the addition of AERO to the BIS Entity List they sold their part number 6130-4 to AERO on

at least three occasions. This part is a blade antenna. CCA's website lists the applications for these blade antennas as:

- Data Links, Telemetry, Transponder
- Aircraft
- UAVs
- Helicopters
- Tactical Missiles
- Ships
- Ground-Based Vehicles
- Single or Array Implementations with Matching Power Dividers and Cables

23. The particular model, 6130-4, operates in the "S-band." According to the defense contractor Cobham's website "The S-band (2-4GHz) frequency is used for satellite communication and radar. It is used by the shipping, aviation and space industries for its efficiency as a conduit for supplying vital real-time data and for high resilience to rain fade and other environmental interference.[2]

24. In March of 2019, CCA reported to OEE Boston that they received at least three requests for part number 6130-4. Two of the parties that requested these parts were in Pakistan: Engineering Aura of Wah Cantt and Universal Trading Company of Karachi. The third was Electro Power Solutions of Hong Kong. In October of 2019 a grand jury in New Hampshire indicted, amongst others, Muhammad Ashraf Khan of Hong Kong for conspiracy to violate IEEPA and ECRA in part because of his use of Electro-Power Solutions in Hong Kong to divert US-origin commodities to prohibited end users in Pakistan, including AERO. In January of 2020, the US Department of Commerce issued a Temporary Denial Order against, amongst

[2] From https://sync.cobham.com/satcom/knowledge-library/getting-started-on-satellite-communications/what-is-s-band/ accessed on July 28, 2020

others, Muhammad Ashraf Khan and Electro-Power Solutions. This order prohibited these entities from receiving US exports on a temporary basis because of their role in diverting US origin goods to prohibited entities in Pakistan, including AERO.

25. Review of emails from the previous search warrant returns contain an email from procurement.log@gmail.com that was sent on March 14, 2019. Review of the email header information shows that there were multiple recipients including "RAMTECH" utilizing huma@ramtech.com.pk and "SPEAR TECHNOLOGIES" utilizing TA. The email's subject is listed as "TE-000717-18-19."

26. I know from my prior involvement in the investigation into illicit procurement by AERO as well as the review of numerous AERO emails, that this subject is consistent with how AERO labels and distributes a specific tender. A tender is essentially an invitation to various parties to bid on, or provide a quote for a specific desired part or commodity.

27. Review of this March 14, 2019 email contains a message that says the following:

> "Dear Sir
> Enclosed please find our subject tender enquiry.
> Regards
> Tendering Section
> Logistics Dte"

28. Attached to the email is a document titled "TE-000717-18-19." Review of this document reveals a Request for Quote dated March 13, 2019. The Request for Quote is from "United Enterprises" and lists an address of "Mohra Chowk, Hazara Road, Hassan Abdal, Distict Attock, Pakistan." The document goes on to read that "United Enterprises intends to buy the undermentioned store on CPT Islamabad basis." The item description is listed as "Antena; Blade 2.30-2.5GHz 350W P/N 6130-4, Manufacturer: HAIGH-FARR, OEM PART NO.:6130-4" and lists a quantity of "125 EA."

29. Beginning in at least January 2014, AERO and Integrated Solutions, a company added to the BIS Entity List on January 26, 2018 as an alias for AERO, has used procurement.log@gmail.com to send out tenders to their procurement network for items they are seeking to acquire.

30. Beginning in at least April 2018, procurement.log@gmail.com began sending out tenders utilizing a company called "United Enterprises" and an address of "Mohra Chowk, Hazara Road, Hassan Abdal, District Attock, Pakistan." The format of United Enterprises tender forms appears identical to the tender forms that included AERO and Integrated Solutions previously. I have personally reviewed over one-hundred (100) separate tenders or Requests for Quote sent from procurement.log@gmail.com that utilize "United Enterprises" with the same or similar address.

31. In addition, beginning on at least January 18, 2018, a company located in the United Kingdom called "Buziness World" received a Purchase Order number PO-000461-17-18 from procurement.log@gmail.com that shows the purchasing party as "United Enterprises." In January 2020, the US Department of Commerce issued a Temporary Denial Order against, amongst others, "Buziness World." The format of the United Enterprise's Purchase Order form appears identical to purchase orders that were issued by AERO and Integrated Solutions. The address for United Enterprises is the same as well: Hohra Chowk, Hazara Road, Hasan Abdal, District Attock, Pakistan.

32. In September of 2019 a man named Zafar Iqbal of Tinca, Inc. in Sterling, VA requested 50 of blade antenna part number 6130-4 from CCA. Zafar told CCA that the end use of the antennas was for race cars (the CCA website references race cars as a use for some blade antennas). OEE agents spoke with Zafar in May of 2020. He told the agents that he acquires

items for a company called Alpial FZC in the UAE who then sends the commodities to Pakistan but he doesn't know who the end user is. A check of UAE business registrations reveals that Alpial Associates LLC FZ is registered in the UAE in the Ras Al Kaimah Economic Zone. According to the website of the Ras Al Kaimah Economic Zone, rakez.com, the zone consists of one building.

33. On or about July 21, 2020 CCA again received correspondence from Engineering Aura of Wah Cantt, Pakistan. This e-mail, signed by "Rehan Feroze," was a follow up to the correspondence in March of 2019. Feroze told representatives of CCA that he wished to purchase 125 blade antennas, CCA part number 6130-4.

34. I know from my prior involvement in the investigation into illicit procurement by AERO and its network of procurement agents that this time frame is consistent with how AERO frequently operates. It is the normal course of business for a tender to stay open for many months before a purchase order is awarded to the selected party.

35. Review of emails from the previous search warrant return reveals an email sent to TA from "ABC DEF" utilizing procurement301983@gmail.com on or about July 22, 2020. The email's subject reads "QUOTATION REQUIRED" and the email states:

> "Dear Sir,
>
> Please forward your quote for the under mentioned item at the earliest.
>
> ROUNDED BLADE ANTENA; 2.30-2.5GHz 350W,
> AVERAGE POWER AROUND 15W CW
> Manufacturer; [CCA]
> OEM PART NO. 6130-4
>
> QTY – 125 EA
>
> Regards
> Manager Procurement
> Cell No 92 0320 7281037

LL No 92 051 9018 2337"

36. On or about the same day Omair Awan received this email, he forwarded it utilizing TA, to rakhmangul@gmail.com.

37. Then, again on or about the same day of July 22, 2020, CCA was contacted by "Rakhman Gul" the Chief Executive Officer of Ramtech, ostensibly a company in Islamabad, Pakistan. This request came from rakhmangul@gmail.com. Gul was requesting 125 units of CCA blade antenna, part number 6130-4.

38. On or about August 5, 2020, TA emailed procurement301983@gmail.com and saghirkhattak@gmail.com. The subject of the email reads "Re: QUOTATION REQUIRED" and the email states:

> "Dear Sir,
>
> Attached please find commercial quotation for your perusal. Please note that since these items are of critical nature and since we have received the End User Certificate so we would request your good office to expedite the process of issuance of PO or provide us with LOI so that there shall not be any delay which will obviously hamper the process or may lead to rejection of end user eventually, due to delays.
>
> Regards,
> Omair Awan"

39. On or about August 17, 2020, TA forwarded the above email to "Rakhman Gul" at rakhmangul@gmail.com.

AERO'S ONGOING EFFORT TO ACQUIRE U.S. COMMODITIES

40. Cooperating company B ("CCB") is a defense contractor and manufacturer of thermal and night vision imaging devices headquartered in Wilsonville, OR with satellite offices throughout the United States, including Nashua, NH. On or about March 5, 2020, CCB was

contacted by "Kamran Hasan" utilizing k1hasan@gmail.com requesting a quotation for one (1) wafer of ISC9705 and ISC9901 standard ROICs. According to CCB's website, these ROICs (Read-Out Integrated Circuits) are utilized for building infrared focal plane arrays. At the bottom of the email, Kamran Hasan's signature block read:

> "Cordially,
> Dr. Kamran Hasan
> United Enterprises
> Pakistan"

41. In subsequent email communications, Kamran Hasan discussed with CCB getting separate quotations for each ROIC as well as changing delivery terms from "Exworks" to either "FOB" or "CPT." CCB replied and among other things, stated that they cannot change delivery terms. On or about April 20, 2020, Kamran Hasan replied to CCB's previous email, this time including rakhmangul@gmail.com in the "Cc" line. Kamran Hasan wrote:

> "Hello [CCB employee],
>
> Thank you for your email and quotation. Since you have provided the quotation with advance payment terms, but our company doesn't allow to make advance payments. Therefore, we will follow the same procedure which we opted for our last purchase in 2011. We want to engage Spear Technology to complete the procurement for us. The contact person will be Mr Rehman Gul and his email address is in cc. He will contact you for further correspondence. He will also provide you all the required documentation for export license. In first purchase, we will initiate the procurement process of quotation for ISC9901 640x512 format ROICs (part#406-9901-50-01). Thanks a lot for your support and cooperation.
>
> With my best regards,
> Dr. Kamran"

42. On or about the same day, April 20, 2020, shortly after sending this email, Kamran Hasan, utilizing k1hasan@gmail.com, sent an email to rakhmangul@gmail.com with mshussain76@gmail.com in the "Cc" line. The email read:

"Please send the following documents (reference to telephonic conversation with Dr. Sajid Hussain);
1. Quotation
2. Documents required for export license
3. Standard terms and conditions"

43. Rakhmangul@gmail.com then forwarded this same message to TA on or about April 21, 2020.

44. On or about April 23, 2020, rakhmangul@gmail.com sent an email to TA with a subject of "Company Profile." In the email, Rakhman Gul asked TA to look at the attached profile and to "please go through it with a critical eye, make corrections and if anything or idea is missing, add on to it." This email included an attachment labeled "RAMTECH Profile New 2020." The attachment is a two-page word document on RAMTECH letterhead and is titled "Company Profile."

45. The document states that RAMTECH is "an Islamabad based Company that was formed in 2014 with a mission statement to Continuously Endeavor Towards Becoming a Reliable Logistic Support Integrator within the Supply Chain of Customers." It continues on to state that "RAMTECH holds offices in China, UAE and Germany by the names of Diqun Industrial Co. Ltd, Spear Technologies and Solar-B respectively." The document also states that "RAMTECH's business portfolio includes Integrated Logistic Support to the Defense Industry and the Armed Forces, Facilitation of Partnerships for development, qualification and manufacturing of Critical Sub-Systems of Operational Platforms, Provision of Developmental Tools, machinery and Spares Support (mil-spec and industrial grade connectors, wires and other robust electronics) to the Industry."

46. This document also includes a paragraph that states "Given the nature of business, RAMTECH has to, off and on, undergo security clearance by various security agencies in

Pakistan. RAMTECH is currently security cleared to undertake business with Directorate General Defense Production, Pakistan Ordnance Factories, Advanced Engineering Research Organization and DESTO (SPD)."

47. DESTO, or the Defense Science and Technology Organization is also included on the BIS Entity list, being added in November 1998, and amended in September 2012 to include the aliases "Defense Science and Technology Center" and "Chaklala Defense Science and Technology Organization."[3]

48. The RAMTECH Company Profile also lists Rakhman Gul as the "Chief Executive Officer" and Omair Ahmed Awan as one of the Electrical Engineers that has been working with RAMTECH since 2015.

49. On or about April 27, 2020, Rakhman Gul, utilizing rakhmangul@gmail.com, emailed CCB:

> "Hi [CCB employee],
> My apologies for the delay in reply.
> My name is Rakhman Gul. I've been asked by Dr. Kamran to facilitate the procurement of ISC9901 640x512 format ROIC's from you. My Company "Spear Technologies General Trading LLC" is based in Fujairah, UAE. However, since it is a free zone company, I handle most of its operations from Pakistan. Given below are the details of the Company.
> Company Name: Spear Technologies General Trading LLC
> Company Address: Postal: Office 1104, 11th Floor PO Box 7800, Fujairah, UAE
> For telephonic contact please use +92-300-5354324. For email correspondence use rakhmangul@gmail.com.
> Please send across the quote along with the required/necessary terms and conditions to enable the facilitation of the procurement process as well as the receipt of goods by the customer.
>
> Best Regards
> RG"

[3] As published in The Federal Register on November 19, 1998, 63 FR 64322 and on September 19, 2012, 77 FR 58006 (no. 182) respectively.

50. On or about May 4, 2020, "Sajid Hussain," utilizing mshussain76@gmail.com, sent an email to rakhmangul@gmail.com and Cc'd "Dr. Mohammad Shafi" (shafi3974@gmail.com). In the email, Sajid Hussain told Rakhman Gul that "I hope this email finds you well. I am waiting for your reply regarding any update of the project. with my best regards, Dr. Sajid"

51. On or about May 6, 2020, a Compliance Paralegal from CCB emailed rakhmangul@gmail.com and asked him to complete a due diligence questionnaire. On or about May 7, 2020, rakhmangul@gmail.com forwarded this email to k1hasan@gmail.com and mshussain76@gmail.com and stated "Have filled up the forms and submitted. Let's see what they say"

52. In a subsequent email, CCB also requested Rakhman Gul to provide a copy of a business license for Spear Technologies. Rakhman Gul, utilizing rakhmangul@gmail.com sent an email on or about May 23, 2020 with two attachments which he described as "license renewals." A review of those attachments show that they appear to be documents produced from the United Arab Emirate's Government of Fujairah's International Free Zone Authority. Among other information, the document shows an incorporation date of March 4, 2019 for Spear Technologies General Trading LLC and lists both the owner and general manager for the company as "Omair Ahmed Awan."

53. On or about July 21, 2020, CCB sent Kamran Hasan and Rakhman Gul a form to be filled out that includes information related to the end user and end use of the product, contact and address information, consignee information if different from the purchasing party, as well as any other third party information that would be related to the transaction. On or about July 21, 2020, Rakhman Gul forwarded this message to k1hasan@gmail.com and said "Dear Sir, [CCB

employee] has asked for filling of the form. They understand United Enterprises to be the End User. The same form will be used for getting an Export license. Please advise." On or about July 23, 2020, rakhmangul@gmail.com also forwarded the July 21, 2020 email from CCB to mshussain76@gmail.com and included the original form from CCB in an attachment.

54. On or about July 29, 2020, "Sikandar Zulqarnain," utilizing sikandar.iat@gmail.com, sent an email to rakhmangul@gmail.com with mshussain76 and shafi3974@gmail.com Cc'd. The email reads:

> "Dear Sir
> Rehman Gul Sb.
> Assalamu Alekum
> Hope you are fine and doing well. I am writing this email with reference to today's telephonic conversation with Dr. Sajid Hussain. Sir, to proceed the approval process for procurement of ROICs please find the filled copy of [CCB] form in the attachment.
> Thanking you for your kind cooperation.
> Best Regards.
> Sikandar."

The email also includes an attachment with the same form that CCB originally provided to klhasan@gmail.com and rakhmangul@gmail.com. However, this time the form that is being provided to Rakhman Gul, has portions of the end user and end use section filled in. Included in this section are boxes that say either yes or no to the question of military end user or military end use. For both of these questions, the boxes are now checked as "No." The section that asks about the nature of the business now lists "Security surveillance solution providers for civic and domestic applications." The form also asks for a detailed description of the intended end use of the product. In this section, the form now reads "The intended end use of the product is only for civic purpose applications. Thermal imagers will be used for surveillance only i.e. security surveillance and thermography for medical applications."

55. In my training and experience, front-companies or third party companies that are

used for the procurement of products often seek guidance from the true end-user or customer in order to provide information or fill out forms such as the one CCB provided. Additionally, it is common for military end-users, i.e. AERO, to hide the fact that a product has a military end-use when purchasing from U.S. manufacturers.

56. On or about August 5, 2020, Rakhman Gul emailed CCB and Cc'd TA. The email stated "Attached the document as required by you" and included the same CCB form attached. This time, the form was filled out more completely. It listed the purchasing party as "Spear Technologies General Trading, LLC" and the contact person as "Rakhman Gul (Consultant)." It listed the product description and quantity as "ISC9901, 640x512 format, 20micron pitch ROICs. Part No. 406-9901-50-01, Qty. 54."

57. The form now listed the end user as "RAMTECH" with an address of "No 60, Street 4, G-15/4, Islamabad, Pakistan." The contact person listed for Ramtech is "Rakhman Gul" and lists rakhmangul@gmail.com as well as info@ramtech.com.pk as email addresses. The military end user and end use boxes are still checked "No" but the "Nature of Business" section is now slightly different. It now reads "Developmental Work on Test Equipment, Consultancy on Test and Evaluation of Products, Supply of Equipment, Partnership in Security Surveillance Solution Providers for Civic and Domestic Applications." The section that asks for a detailed description of the intended use of the product has the same information from when sikandar.iat@gmail.com previously sent the filled form back to Rakhman Gul. The consignee is also listed as "RAMTECH." There is no information provided in the section that asks about third parties.

ASSOCIATION OF TA WITH AERO AND ITS ALIAS COMPANIES

58. Review of AERO emails reveals that TA has been receiving emails directly from

procurement.log@gmail.com since as early as May 2017. These emails contain hundreds of Tenders from Integrated Solutions and other AERO alias companies as well as Purchase Orders through TA's associated company "Spear Technologies."

59. As recently as on or about August 12, 2020, procurement.log@gmail.com sent an email to TA and others. This email read "Dear sir Enclosed please find our subject tender enquiry. Regards Tendering Section Logistics Dte." The email includes an attachment named "IT20-000067." The document is an "Invitation for Tender" and includes several parts from various companies throughout the world. One of the parts references a specific hardware, "Nut; Self Lock M5 P/N 5PH35M" and a manufacturer that is based in Corona, CA. The Tender is utilizing a company named "Quantum Logix (Private) Limited" located at "Plot No 22, Sector H-9, Islamabad." Based on the layout of the tender as well as it being sent from procurement.log@gmail.com, "Quantum Logix (Private) Limited" appears to be a new alias company for AERO.

60. Based on my experience in past investigations involving AERO, as well as the review of hundreds of emails contained in the previous search warrant returns, AERO utilizes a number of trusted procurement agents in order to fulfill their requests. Their typical course of business generally includes first sending a Tender out to their procurement network via email, receiving quotes back from individuals or companies wishing to bid as a supplier, and ultimately issuing a Purchase Order to trigger the procurement agent's further pursuit of that product.

PRESERVATION OF EVIDENCE

61. On or about September 24, 2020, pursuant to 18 U.S.C. § 2703(f)(1), a preservation request letter was sent to Microsoft for omairawan@hotmail.com (TA).

TECHNICAL BACKGROUND

62. In my training and experience, I have learned that Microsoft provides a variety of online services, including e-mail access, to the public. Microsoft allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the Target accounts. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, Microsoft's computers are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

63. Microsoft e-mail subscribers can access their accounts on servers maintained and/or owned by Microsoft from any computer connected to the Internet located anywhere in the world. E-mail messages and files sent to a Microsoft account are stored in the account's "inbox" as long as they are not identified as "junk mail," the account has not exceeded the maximum storage limit, or the account is not set up to forward messages to another e-mail account. If the message/file is not deleted by the subscriber, the account is below the maximum storage limit, and the account has not been inactivated, then the message/file will remain on the server indefinitely. E-mail messages and files sent from a Microsoft account will remain on the server unless the account user changes the default account settings.

64. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If a Microsoft e-mail user writes a draft message but does not send it, that message may also be saved by Microsoft but may not include all of these categories of data.

65. In my training and experience, in addition to e-mails, Microsoft subscribers can also store files such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Microsoft. Evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

66. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

67. This application seeks a warrant to search all responsive records and information under the control of Microsoft, a provider subject to the jurisdiction of this court, regardless of where Microsoft has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Microsoft's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. (See 18 U.S.C. § 2713)

FOURTEEN-DAY RULE FOR EXECUTION OF WARRANT

68. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the

Court issues this warrant, the United States will execute it not by entering the premises of Microsoft, as with a conventional warrant, but rather by serving a copy of the warrant on the company and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

69. Based on my training and experience and that of other law enforcement, I understand that e-mail providers sometimes produce data in response to a search warrant outside the 14-day period set forth in Rule 41 for execution of a warrant. I also understand that e-mail providers sometimes produce data that was created or received after this 14-day deadline ("late-created data").

70. The United States does not ask for this extra data or participate in its production.

71. Should Microsoft produce late-created data in response to this warrant, I request permission to view all late-created data that was created by Microsoft, including subscriber, IP address, logging, and other transactional data, without further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail communications, absent a follow-up warrant.

72. For these reasons, I request that the Court approve the procedures in Attachment B, which set forth these limitations.

CONCLUSION

73. In light of the fact that AERO and its alias companies have employed TA to facilitate the acquisition of US origin commodities and that this account has had communications

regarding this ongoing attempted procurement as recent as August 2020, probable cause exists that this account is still being used for such acquisitions.

74. Accordingly, there is probable cause to believe that records and data from the Target Account (as described in Attachment A), contain evidence, fruits, and instrumentalities of the above-listed crimes (as described in Attachment B).

75. The procedures for copying and reviewing the relevant records are set out in Attachment B to the search warrant.

Respectfully submitted

/s/ Jon P. Bentsen
Jon P. Bentsen
Special Agent
Office of Export Enforcement
Bureau of Industry and Security
United States Department of Commerce

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: November 10, 2020
Time: **4:53 PM, Nov 10, 2020**

Andrea K. Johnstone,
United States Magistrate Judge

ATTACHMENT A

The premises to be searched and seized is (1) the e-mail account identified as omairawan@hotmail.com (TA) ("the Target Account"), (2) other user-generated data stored with the Target Account, and (3) associated subscriber, transactional, user connection information associated with the Target Account, as described further in Attachment B. This information is maintained by Microsoft, Inc. ("Microsoft"), which accepts service of process at 1025 La Avenida, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 24, 2020, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of the Subject Offenses (International Emergency Economic Powers Act, 50 U.S.C. §§ 1702 and 1705; the Export Control Reform Act, 50 USC § 4819 13 U.S.C; 13 U.S.C. § 305 (unlawful export information activities), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 554 (outbound smuggling), 18 U.S.C. § 1001 (false statements), and 18 U.S.C. § 1956 (money laundering)) for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Records and information related to violations of the aforementioned statutes and regulations;

(b) Records and information related to any purchases, sales, or requests for purchase or sale of U.S.-origin goods or export-controlled items;

(c) Records and information related to payments for any U.S.-origin goods or suspected export-controlled items, including bank records, wire transfers, checks, credit card bills, account information, other payment websites, or other financial records;

(d) Records and information related to any shipping, delivery, or customs declaration of U.S.-origin goods or export-controlled items;

(e) Records and information related to actual or potential buyers and sellers of U.S.-origin goods or export-controlled items, including biographical information, addresses, e-mail addresses, user names, social security numbers, or other pertinent identifying information;

(f) Records and information related to the identity and whereabouts of any of the individuals or entities associated with the Target Account, including biographical information, addresses, e-mail addresses, user names, social security numbers, or other pertinent identifying information;

(g) Records and information related to the use or planned use of U.S.-origin goods or export-controlled items;

(h) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner; and

(i) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

CERTIFICATE OF AUTHENTICITY

I, _____, attest, under penalties of perjury, that the information contained in this declaration is true and correct. I am employed by Microsoft, Inc., and my official title is _____. I am a custodian of records for Microsoft, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Microsoft, Inc., and that I am the custodian of the attached records consisting of _____ (folders/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Microsoft, Inc.; and

c. such records were made by Microsoft, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature